

CÓMO PROTEGERSE DE LAS AMENAZAS

Las 10 recomendaciones del Centro de Alerta Temprana, dependiente del Ministerio de Ciencia y Tecnología, para mantener 'limpios' los equipos informáticos:

USAR UN ANTIVIRUS ACTUALIZADO

Utiliza un antivirus que se actualice periódicamente, en segundo plano y en cada sesión, ya que para que un antivirus sea eficaz necesita conocer la *firma* y las características de los nuevos virus que van surgiendo. Un antivirus es un programa informático específicamente diseñado para detectar y eliminar virus. Es conveniente tener uno instalado en el ordenador y programarlo para que revise todo el equipo de forma periódica. Verifica también regularmente que el antivirus está activo, dado que algunos virus detienen los programas de protección y dejan a su ordenador indefenso frente a otros ataques.

INSTALAR UN FIREWALL

Indispensable para conectarse a Internet con ADSL. Un cortafuegos o *firewall* es un programa de *software* destinado a garantizar la seguridad en las comunicaciones a través de Internet. Su cometido consiste en bloquear las entradas no autorizadas a tu ordenador y restringir la salida de información sin permiso. Instala un programa de este tipo si dispones de conexión permanente a la Red, por ejemplo mediante ADSL y, sobre todo, si tu dirección IP es fija.

INSTALAR TODOS LOS PARCHES DE SEGURIDAD

Los fallos de seguridad que se detectan en los programas informáticos más utilizados, tales como los sistemas operativos, navegadores, procesadores de texto, programas de correo, etc. son el blanco habitual de los creadores de virus. Cuando se detecta un fallo, que hace que el ordenador del cliente sea vulnerable, las compañías fabricantes del software ofrecen rápidamente a través de Internet actualizaciones, llamadas parches de seguridad. Las aplicaciones más extendidas te informarán de que están disponibles actualizaciones disponibles. Si no fuese así, es conveniente visitar periódicamente los sitios web de estas compañías e instalar las actualizaciones más recientes.

INSTALAR SÓLO SOFTWARE LEGAL

Es muy recomendable que todo el *software* instalado en tu ordenador provenga de una fuente legítima y segura. Las copias pirata de los programas propietarios son potencialmente peligrosas. Además de transgredir la ley, pueden contener virus, *spyware* o archivos de sistema incompatibles con los de tu ordenador, lo cual provocará inestabilidad en tu equipo. A veces, los programas desprotegidos que se descargan de algunos sitios *web*, son una vía de propagación de virus. Es mucho más aconsejable instalar software libre y de código abierto, que es legítimo y nadie tiene necesidad de desprotegerlo para copiarlo. En cualquier caso, debes analizar con un antivirus cualquier fichero que te descargues de Internet.

TOMAR PRECAUCIONES CON EL CORREO ELECTRÓNICO

Antes de abrir un mensaje cualquiera, es conveniente leer el encabezado de todos los correos electrónicos recibidos. Debes sospechar de los mensajes **sin asunto**, los que están redactados en **idiomas distintos** al nuestro, los que tienen un **Asunto** poco claro y de los mensajes **no esperados**, incluso si provienen de algún conocido. En caso de duda, llama por teléfono al remitente para asegurarte. Los virus utilizan la libreta de direcciones de los ordenadores que ya han infectado para enviar sus réplicas y tratar de contagiar a otros usuarios haciéndoles creer que están recibiendo un mensaje de un remitente de confianza.

NO ABRIR ARCHIVOS NO SOLICITADOS

No se debe aceptar la descarga de ficheros ejecutables, documentos, etcétera, que no hayan sido solicitados. Si quieres incorporar a tu ordenador un nuevo elemento, debes revisarlo con una aplicación antivirus. No abras ningún archivo con doble extensión, por ejemplo archivo.**txt.vbs** porque, en condiciones normales, no tendrías que necesitar nunca este tipo de ficheros. Configura tu sistema para que muestre las extensiones de todos los archivos desde el **Panel de Control / Opciones de Carpeta / Ver**.

HAZ COPIAS DE SEGURIDAD FRECUENTES

Es muy conveniente realizar, de forma periódica, copias de seguridad de la información más valiosa de tu disco duro. No dudes incluso en hacer doble copia de seguridad y mantener la copia que hiciste anteriormente. En caso de sufrir un ataque de un virus, una intrusión o una avería general de tu ordenador, las secuelas serán mucho menores si puedes restaurar fácilmente tus datos al estado que tenían en la última copia de seguridad que hiciste.

NO SEAS OTRO ESLABÓN DE LA CADENA

No ayudes a la extensión del **malware**. No distribuyas indiscriminadamente bromas de virus, alarmas o cartas en cadena. No reenvíes mensajes piramidales. Remite una copia del **malware** que te llegue a centros especializados en seguridad, como el Centro de Alerta Antivirus. Infórmate de la veracidad de los mensajes recibidos y ayuda a los demás internautas colaborando en la detención de su distribución. No contestes a **ninguno** de los mensajes de *spam* que recibas, ya que al hacerlo estarás confirmando que tu dirección de correo es válida.

MANTENTE INFORMADO

Suscríbete a boletines de noticias sobre seguridad. Recibir información periódica sobre las novedades de seguridad informática puede ser muy útil. Los boletines de las compañías fabricantes de software son el medio ideal para hacerlo, así como de los servicios de información y boletines del **Centro de Alerta Antivirus** o en las web especializadas como **Criptonomicon**. Estar informado sobre cómo actuar ante una situación de riesgo, podrá minimizar las posibles pérdidas.

BORRA TODOS LOS ARCHIVOS SOSPECHOSOS

Todos aquellos correos electrónicos que resulten sospechosos, de los que desconoces el remitente o presentan un **Asunto** extraño, que puede ser una trampa o percha para virus, deben ir a la papelera. A continuación, no hay que olvidar vaciarla porque, al fin y al cabo, la papelera es una carpeta más del sistema.